

141**VYHLÁŠKA**

ze dne 26. června 2018

**o hlášení závažných bezpečnostních a provozních incidentů
osobami oprávněnými poskytovat platební služby**

Česká národní banka stanoví podle § 263 zákona č. 370/2017 Sb., o platebním styku, k provedení § 221 odst. 5:

§ 1**Předmět úpravy**

Tato vyhláška stanoví podrobnosti náležitostí oznámení závažného bezpečnostního nebo provozního incidentu v oblasti platebního styku (dále jen „oznámení“), jeho formáty a další technické náležitosti při hlášení závažných bezpečnostních a provozních incidentů v oblasti platebního styku osobami oprávněnými poskytovat platební služby.

§ 2**Oznámení**

Osoba oprávněná poskytovat platební služby předkládá České národní bance oznámení zahrnující v části

- a) A úvodní oznámení,
- b) B průběžné oznámení a
- c) C závěrečné oznámení.

§ 3**Podrobnosti náležitostí oznámení**

Osoba oprávněná poskytovat platební služby podává oznámení na formuláři, jehož vzor je uveden v příloze č. 1 k této vyhlášce, a postupně do něj doplňuje údaje do jednotlivých částí podle § 2.

§ 4**Formát a další technické náležitosti oznámení**

- (1) Oznámení se podává ve formátu xls/xlsx.
- (2) Oznámení jsou České národní bance předávána prostřednictvím internetového rozhraní České národní banky pro sběr informačních povinností a výkazů.
- (3) Oznámení lze učinit také v anglickém jazyce. Vzor formuláře v anglickém jazyce je uveden v příloze č. 2 k této vyhlášce

§ 5**Účinnost**

Tato vyhláška nabývá účinnosti dnem 1. srpna 2018.

Guvernér:

Ing. Rusnok v. r.

B – Průběžné oznámení			
B 1 – OBEČNÉ ÚDAJE			
Uveďte prosím PODROBNĚJŠÍ popis incidentu, např. následující informace: a) v čem je konkrétně problém b) jak k němu došlo c) jak se vyvíjel d) souvisel s některým předchozím incidentem e) důsledky (zejména pro uživatele platebních služeb) f) základní informace o zjištění incidentu g) dotčené oblasti h) dosud přijatá opatření i) dotčení nebo zúčastnění poskytovatele služeb / třetí strany j) zahájení krizového řízení (interně a/nebo externě (krizové řízení centrální banky)) k) interní klasifikace incidentu podle osoby oprávněné poskytovat platební služby			
Datum a čas vzniku incidentu (je-li již informace k dispozici)	DD/MM/RRRR, HH:MM		
Stav incidentu	☐ Diagnostika ☐ Obnova ☐ Oprava ☐ Opětorné zahájení provozu		
Datum a čas, kdy během incidentu došlo nebo podle očekávání dojde k návratu do původního stavu	DD/MM/RRRR, HH:MM		
B 2 – KLASIFIKACE INCIDENTU A INFORMACE O INCIDENTU			
Celkový dopad	☐ Integrita ☐ Důvěrnost ☐ Kontinuita ☐ Dostupnost ☐ Autenticita		
Dotčené transakce ⁽²⁾	Počet dotčených transakcí Jako procentuální podíl z běžného počtu transakcí Hodnota dotčených transakcí v eurech Poznámky: ☐ Skutečný údaj ☐ Odhad ☐ Skutečný údaj ☐ Odhad ☐ Skutečný údaj ☐ Odhad		
Dotčení uživatelů platebních služeb ⁽³⁾	Počet dotčených uživatelů platebních služeb Jako procentuální podíl z celkového počtu uživatelů platebních služeb ☐ Skutečný údaj ☐ Odhad ☐ Skutečný údaj ☐ Odhad		
Délka výpadku služby ⁽⁴⁾	Celková délka výpadku služby DD:HH:MM ☐ Skutečný údaj ☐ Odhad		
Ekonomický dopad ⁽⁵⁾	Přímé náklady v eurech Nepřímé náklady v eurech ☐ Skutečný údaj ☐ Odhad ☐ Skutečný údaj ☐ Odhad		
Vysoká úroveň interní eskalace	☐ ANO ☐ ANO A PRAVDĚPODOBNĚ DOJDE K VYHLÁŠENÍ KRIZOVÉHO (NEBO PODOBNÉHO) REŽIMU ☐ NE Popište úroveň interní eskalace incidentu a uveďte, zda incident vedl nebo pravděpodobně povede k vyhlášení krizového (nebo podobného) režimu, a pokud ano, uveďte popis		
Další potenciálně dotčené osoby oprávněné poskytovat platební služby nebo související infrastruktury	☐ ANO ☐ NE Popište, jak by incident mohli ovlivnit jiné osoby oprávněné poskytovat platební služby a/nebo infrastruktury		
Reputační dopad	☐ ANO ☐ NE Popište, jak by incident mohli ovlivnit reputační dopad na osoby oprávněné poskytovat platební služby (např. mediální pokrytí, potenciální porušení právních nebo regulačních povinností atd.)		
B 3 – POPIS INCIDENTU			
Druh incidentu	☐ Provozní ☐ Bezpečnostní		
Příčina incidentu	☐ Probíhá šetření ☐ Externí útok ☐ Interní útok ☐ Externí událost ☐ Lidská chyba ☐ Selhání procesu ☐ Selhání systému ☐ Jiné ☐ Druh útoku: ☐ Distribuované odepření služby / odepření služby (D/DoS) ☐ Nákaza interních systémů ☐ Cílený průnik ☐ Jiné Je-li zvoleno „jiné“, specifikujte:		
Dotkl se váš incident přímo nebo prostřednictvím poskytovatele služeb?	☐ Přímě ☐ Nepřímě Pokud nepřímě, uveďte jméno poskytovatele služeb		
B 4 – DOPAD INCIDENTU			
Případné dotčené budovy (adresy)			
Dotčené obchodní kanály	☐ Pobočky ☐ Telefonní bankovníctví ☐ Místo prodeje ☐ Elektronické bankovníctví ☐ Mobilní bankovníctví ☐ Jiné ☐ Bankomaty		
Dotčené platební služby	☐ Vložení hotovosti na platební účet ☐ Úhrada ☐ Poukazování peněz ☐ Výběr hotovosti z platebního účtu ☐ Inkaso ☐ Služby iniciování platby ☐ Operace nutné pro vedení platebního účtu ☐ Platby kartou ☐ Služby informování o účtu ☐ Pořizování platebních prostředků ☐ Vydávání platebních prostředků ☐ Jiné		
Dotčené funkční oblasti	☐ Ověřování/autorizace ☐ Žitčování ☐ Nepřímé vypořádání ☐ Komunikace ☐ Přímé vypořádání ☐ Jiné		
Dotčené systémy a složky	☐ Aplikace/software ☐ Hardware ☐ Databáze ☐ Sítí/infrastruktura ☐ Jiné		
Dotčení pracovníci	☐ ANO ☐ NE Popište, jak by se incident mohli dotknout pracovníků osoby oprávněné poskytovat platební služby či poskytovatele služeb (např. pracovníci se nemohli dostat do kanceláře a poskytovat zázakníkům podporu atd.)		
B 5 – ZMÍRNĚNÍ INCIDENTU			
Jaká opatření byla doposud přijata nebo jsou plánována s cílem dosáhnout obnovy v případě incidentu?			
Došlo k aktivaci plánů zachování provozu a/nebo plánů obnovy činnosti po havárii?	☐ ANO ☐ NE		
Pokud ano, kdy?	DD/MM/RRRR, HH:MM		
Pokud ano, uveďte popis			
Zrušil nebo oslabil osoba oprávněná poskytovat platební služby v důsledku incidentu některé kontroly?	☐ ANO ☐ NE		
Pokud ano, vysvětlíte			

C – Závěrečné oznámení	
Nebylo-li žádné průběžné oznámení zasláno, vyplňte rovněž oddíl B	
C 1 – OBECNÉ ÚDAJE	
Actualizace informací z průběžného oznámení (shrnutí): a) další opatření přijatá za účelem obnovy v případě incidentu b) přijatá konečná nápravná opatření c) analýza příčin d) získané zkušenosti e) další opatření f) případně další příslušné informace	DD/MM/RRRR, HH/MM
Jestliže osoba oprávněná poskytovat platební služby musela kvůli incidentu zrušit nebo oslabit některé kontroly, jsou původní kontroly opět zavedeny? Pokud ano, vysvětlte	☐ ANO NE
C 2 – ANALÝZA PŘÍČIN A NÁSLEDNÁ OPATŘENÍ	
Co bylo příčinou (je-li již příčina známa)? (je možné přiložit soubor s podrobnými informacemi)	
Hlavní nápravná opatření přijatá nebo plánovaná s cílem zabránit opakování incidentu v budoucnu, pokud jsou již tato opatření známa	
C 3 – DOPLŇUJÍCÍ INFORMACE	
Byly o incidentu informovány další osoby oprávněné poskytovat platební služby? Pokud ano, uveďte bližší informace	☐ ANO NE
Byly proti osobě oprávněné poskytovat platební služby učiněny nějaké právní kroky? Pokud ano, uveďte bližší informace	☐ ANO NE
Poznámky:	
1) Rozevírací nabídka: uživatel platební služby; interní organizace; externí organizace; žádná z výše uvedených možností	
2) Rozevírací nabídka: > 10 % běžné úrovně transakcí a > 100 000 EUR; > 25 % běžné úrovně transakcí nebo > 5 mil. EUR; žádná z výše uvedených možností	
3) Rozevírací nabídka: > 5 000 a > 10 % uživatelů platebních služeb; > 50 000 nebo > 25 % uživatelů platebních služeb; žádná z výše uvedených možností	
4) Rozevírací nabídka: > 2 hodiny; < 2 hodiny	
5) Rozevírací nabídka: > Max (0,1 % kapitálu tier 1, 200 000 EUR) nebo > 5 mil. EUR; žádná z výše uvedených možností	

Reporting template on major incidents
(anglická verze uvedeného dokumentu)

Major Incident Report									
☐ Initial report									
☐ Intermediate report									
☐ Last intermediate report									
☐ Final report									
☐ Incident reclassified as non-major									
Please explain:									
Incident identification number, if applicable (for interim and final reports)		DD/MM/YYYY		Time		HH:MM			
A - Initial report									
A 1 - GENERAL DETAILS									
Type of report	☐ Individual ☐ Consolidated								
Affected payment service provider (PSP)									
PSP name									
PSP unique identification number, if relevant									
PSP authorisation number									
Head of group, if applicable									
Home country									
Country/countries affected by the incident									
Primary contact person				Email		Telephone		Telephone	
Secondary contact person				Email		Telephone		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)									
Name of the reporting entity									
Unique identification number, if relevant									
Authorisation number, if applicable									
Primary contact person				Email		Telephone		Telephone	
Secondary contact person				Email		Telephone		Telephone	
A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION									
Date and time of detection of the incident	DD/MM/YYYY, HH:MM								
The incident was detected by ⁽¹⁾	☐		If Other, please explain:						
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)									
What is the estimated time for the next update?									
DD/MM/YYYY, HH:MM									

B - Intermediate report			
B 1 - GENERAL DETAILS			
Please provide a more DETAILED description of the incident, e.g. information on: a) What is the specific issue? b) How it happened c) How did it develop d) Was it related to a previous incident? e) Consequences (in particular for payment service users) f) Background of the incident detection g) Areas affected h) Actions taken so far i) Service providers/ third party affected or involved j) Crisis management started (internal and/or external (Central Bank Crisis management)) k) PSP internal classification of the incident			
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM		
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration		
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM		
B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT			
Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity		
Transactions affected ⁽²⁾	Number of transactions affected ☐ Actual figure ☐ Estimation As a % of regular number of transactions ☐ Actual figure ☐ Estimation Value of transactions affected in EUR ☐ Actual figure ☐ Estimation Comments:		
Payment service users affected ⁽³⁾	Number of payment service users affected ☐ Actual figure ☐ Estimation As a % of total payment service users ☐ Actual figure ☐ Estimation		
Service downtime ⁽⁴⁾	Total service downtime DD:HH:MM ☐ Actual figure ☐ Estimation		
Economic impact ⁽⁵⁾	Direct costs in EUR ☐ Actual figure ☐ Estimation Indirect costs in EUR ☐ Actual figure ☐ Estimation		
High level of internal escalation	☐ YES YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe		
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures		
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)		
B 3 - INCIDENT DESCRIPTION			
Type of Incident	☐ Operational ☐ Security		
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other If Other, specify		
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly If indirectly, please provide the service provider's name		
B 4 - INCIDENT IMPACT			
Building(s) affected (Address), if applicable			
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs		
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other		
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other		
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other		
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)		
B 5 - INCIDENT MITIGATION			
Which actions/measures have been taken so far or are planned to recover from the incident?			
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated?	☐ YES ☐ NO DD/MM/YYYY, HH:MM		
Has the PSP cancelled or weakened some controls because of the incident?	☐ YES ☐ NO		

C - Final report									
If no intermediate report has been sent, please also complete section B									
C 1 - GENERAL DETAILS									
Please update the information from the intermediate report (summary): a) additional actions/measures taken to recover from the incident b) final remediation actions taken c) root cause analysis d) lessons learnt e) additional actions f) any other relevant information									
Date and time of closing the incident					DD/MM/YYYY, HH:MM				
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place? If so, please explain					☐ YES NO				
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP									
What was the root cause (if already known)? (possible to attach a file with detailed information)									
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known									
C 3 - ADDITIONAL INFORMATION									
Has the incident been shared with other PSPs for information purposes? If so, please provide details					☐ YES NO				
Has any legal action been taken against the PSP? If so, please provide details					☐ YES NO				
Notes:									
(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above									
(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 million; none of the above									
(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above									
(4) Pull-down menu: > 2 hours; < 2 hours									
(5) Pull-down menu: > Max (0.1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above									